RFC-0016 Collaborative Continuous Monitoring Standard

RFC Front Matter

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-09-15
- **Closing Date:** 2025-10-15
- **Short Name:** rfc-0016-collaborative-continuous-monitoring

Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: https://github.com/FedRAMP/community/discussions/87
2. Public Comment Form: https://forms.gle/eMHRbk7TnDBzQsWh7
3. Email: pete@fedramp.gov with the subject "**RFC-0016 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will only be made public when requested by the agency.

Summary & Motivation

Fifteen years ago it was common for a single agency to be the only user of a cloud service for years, leading to the concept of a “sponsor” for FedRAMP - a single agency that would commit to performing expensive and burdensome oversight of a cloud service on behalf of the entire federal government.

Many different agencies with varying missions and use cases now operate the same shared commercial cloud services. Historically, relying on a single agency to oversee a cloud service on behalf of every agency user has created conflict and confusion between agencies, delayed access to new capabilities, and led to unexpected and undesirable security outcomes in some cases.

This proposed Collaborative Continuous Monitoring Standard continues implementing the vision of OMB Memorandum M-24-15 to redesign the government-wide continuous monitoring of cloud services to better align with the requirements of OMB A-130 and the NIST Risk Management Framework. This standard supplements the Significant Change Notification Standard, Vulnerability Detection and Response Standard, and Authorization Data Sharing Standard by adding the following additional requirements and recommendations:

1. Providers are expected to host meetings every 3 months that are open to all agency customers for high-level briefings of changes to the offering.
2. Providers are expected to establish clear lines of support for agency security personnel.
3. Agencies will be able to consume *authorization data* using automation and make ongoing authorization decisions based on *persistently* supplied information filtered for criticality based on their agency use case in accordance with their Information Security Continuous Monitoring plans.

This standard will apply firmly to FedRAMP 20x authorizations when formalized, however application to Rev5 will be optional and may require negotiation between cloud service providers and agencies based on existing customer agreements and expectations.

Effective Date(s) & Overall Applicability

This is a draft standard released for public comment; it does not apply to any FedRAMP authorization and MUST NOT be used in draft form.

- FedRAMP **20x**:
  - This standard will initially apply to all FedRAMP 20x authorizations when formalized.
  - Phase One Pilot participants have one year from authorization to fully implement this standard but must demonstrate continuous quarterly progress.
  - Phase Two Pilot participants must demonstrate significant progress towards implementing this standard prior to authorization.
- FedRAMP **Rev5**:
  - See Balancing FedRAMP Rev5 against improvements to FedRAMP 20x for general information how improved FedRAMP standards will be applied carefully and deliberately to Rev5 authorizations.
  - Rev5 providers should expect to adopt at least the Significant Change Notification Standard and Vulnerability Detection and Response Standard prior to adopting this Balance Improvement Release.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

OMB Circular A-130: Managing Information as a Strategic Resource section 4 (c) states that agencies SHALL *"conduct and document security and privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance"*

The FedRAMP Authorization Act (44 USC § 3609 (a)(1)) directs the Administrator of the General Services Administration to *"develop, coordinate, and implement a process … including, as appropriate, oversight of continuous monitoring of cloud computing products and services"*

Purpose

Agencies are required to continuously monitor all of their information systems following a documented process integrated into their Information Security Continuous Monitoring (ISCM) strategy. These strategies are specific to each agency and may even vary at the bureau, component, or information system levels.

The concept behind collaborative continuous monitoring is unique to government customers and creates a burden for commercial cloud service providers. This standard attempts to minimize this burden by encouraging the use of automated monitoring and review of *authorization data* required by other FedRAMP standards and limiting the expected human interaction costs for cloud service providers and agencies. Agencies are expected to use information from the cloud service provider collaboratively in accordance with their agency ISCM strategy without blocking other agencies from making their own risk-based decisions about ongoing authorization.

Expected Outcomes

- Cloud service providers will operate their services and share additional information with agency customers to ensure they can meet their responsibilities and obligations for safely and securely operating the service

- Federal agencies will have streamlined access to the information they actually need to make ongoing security and authorization decisions while having support from government-wide policies that demonstrate the different responsibilities and obligations for operating cloud services

---

Definitions

FRD-CCM-01

> **Ongoing Authorization Report:** A *regular* report that is supplied by FedRAMP Authorized cloud service providers to agency customers, aligned to the requirements and recommendations in the FedRAMP Collaborative Continuous Monitoring Standard.

FRD-CCM-02

> **Quarterly Review:** A *regular* synchronous meeting hosted by a FedRAMP Authorized cloud service provider for agency customers, aligned to the requirements and recommendations in the FedRAMP Collaborative Continuous Monitoring Standard.

Requirements

FRR-CCM

These requirements and recommendations apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-CCM-01

Providers MUST make an *Ongoing Authorization Report* available to *all necessary parties* every 3 months, in a consistent format that is human readable, covering the entire period since the previous summary; this report MUST include high-level summaries of at least the following information:

1. Changes to *authorization data*
2. Planned changes to *authorization data* during at least the next 3 months
3. *Accepted weaknesses*
4. *Transformative changes*
5. Updated recommendations or best practices for security, configuration, usage, or similar aspects of the *cloud service offering*

FRR-CCM-02

Providers SHOULD establish a *regular* 3 month cycle for *Ongoing Authorization Reports* that does not align with calendar quarters so that reports are spread out during the calendar quarter for agencies.

FRR-CCM-03

Providers MUST publicly include the target date for their next *Ongoing Authorization Report* with the *authorization data* required by FRR-ADS-01.

FRR-CCM-04

Providers MUST establish and share an asynchronous mechanism for *all necessary parties* to provide feedback or ask questions related to each *Ongoing Authorization Report*; all such feedback and questions from agencies, along with responses from the provider, MUST be available to FedRAMP.

FRR-CCM-05

Providers MUST NOT share feedback or questions from agencies publicly or with other parties than FedRAMP UNLESS the agency that submitted the feedback or question approves.

FRR-CCM-06

Providers MUST NOT irresponsibly disclose sensitive information in an *Ongoing Authorization Report* that would *likely* have an adverse effect on the *cloud service offering*.

FRR-CCM-07

Providers MAY responsibly share some or all of the information an *Ongoing Authorization Report* publicly or with other parties if the provider determines doing so will NOT *likely* have an adverse effect on the *cloud service offering.*

FRR-CCM-QR

This section includes requirements and recommendations for providers hosting synchronous *Quarterly Reviews* with all agencies.

FRR-CCM-QR-01

Providers SHOULD host a synchronous *Quarterly Review* every 3 months, open to all necessary parties, to review aspects of the most recent *Ongoing Authorization Report* that the provider determines are of the most relevance to agencies.

FRR-CCM-QR-02

Providers SHOULD regularly schedule *Quarterly Reviews* to occur at least 3 business days after releasing an *Ongoing Authorization Report* AND within 2 weeks of such release.

FRR-CCM-QR-03

Providers MUST NOT irresponsibly disclose sensitive information in a *Quarterly Review* that would *likely* have an adverse effect on the *cloud service offering.*

FRR-CCM-QR-04

Providers MUST include either a registration link or a downloadable calendar file with meeting information for *Quarterly Reviews* in the *authorization data* available to *all necessary parties* required by FRR-ADS-06 and FRR-ADS-07; providers who do not host *Quarterly Reviews* MUST clearly state this and explain this decision in the same *authorization data.*

FRR-CCM-QR-05

Providers hosting *Quarterly Reviews* MUST publicly include the target date for their next *Quarterly Review* with the *authorization data* required by FRR-ADS-01.

FRR-CCM-QR-06

Providers SHOULD include additional information in *Quarterly Reviews* that the provider determines are of interest, use, or otherwise relevant to agencies.

FRR-CCM-QR-07

Providers SHOULD NOT invite third parties to attend *Quarterly Reviews* intended for agencies unless it is of specific relevance; this is because agencies are less likely to actively participate in meetings with third parties.

FRR-CCM-QR-08

Providers MUST NOT disclose feedback or questions from agencies during a *Quarterly Review* with the public or third parties UNLESS the agency that submitted the feedback or question approves.

FRR-CCM-QR-09

Providers SHOULD record or transcribe *Quarterly Reviews* and make such available to *all necessary parties* with other *authorization data* as required by FRR-ADS-06 and FRR-ADS07.

FRR-CCM-QR-10

Providers MAY responsibly share recordings or transcriptions of *Quarterly Reviews* with the public or other parties ONLY if the provider removes all agency information (comments, questions, names, etc.) AND determines sharing will NOT *likely* have an adverse effect on the *cloud service offering.*

FRR-CCM-QR-11

Providers MAY share content prepared for a *Quarterly Review* with the public or other parties if the provider determines doing so will NOT *likely* have an adverse effect on the *cloud service offering.*

Agencies

This section includes requirements and recommendations for agencies who are using FedRAMP Authorized cloud services.

FRR-CCM-AG-01

Agencies MUST review each *Ongoing Authorization Report* to understand how changes to the *cloud service offering* may impact the previously agreed-upon risk tolerance documented in the agency's Authorization to Operate of a federal information system that includes the *cloud service offering* in its boundary.

Note: This is required by 44 USC § 35, OMB A-130, FIPS-200, and M-24-15.

FRR-CCM-AG-02

Agencies SHOULD consider the Security Category noted in their Authorization to Operate of the federal information system that includes the *cloud service offering* in its boundary and assign appropriate information security resources for reviewing *Ongoing Authorization Reports*, attending *Quarterly Reviews*, and other ongoing *authorization data.*

FRR-CCM-AG-03

Agencies SHOULD designate a senior information security official to review *Ongoing Authorization Reports* and represent the agency at *Quarterly Reviews* for *cloud service offerings* included in agency information systems with a Security Category of High.

FRR-CCM-AG-04

Agencies SHOULD formally notify the provider if the information presented in an *Ongoing Authorization Report*, *Quarterly Review*, or other ongoing *authorization data* causes significant concerns that may lead the agency to remove the *cloud service offering* from operation.

FRR-CCM-AG-05

Agencies MUST notify FedRAMP by sending a notification to info@fedramp.gov if the information presented in an *Ongoing Authorization Report*, *Quarterly Review*, or other ongoing *authorization data* causes significant concerns that may lead the agency to stop operation of the *cloud service offering*.

Note: This is an OMB policy; agencies are required to notify FedRAMP in OMB Memorandum M-24-15 section IV (a).

FRR-CCM-AG-06

Agencies SHOULD NOT request additional information from cloud service providers that is not required by this FedRAMP standard UNLESS the head of the agency or an authorized delegate makes a determination that there is a demonstrable need for such.

Note: This is related to the Presumption of Adequacy directed by 44 USC § 3613 (e).

FRR-CCM-AG-07

Agencies MUST inform FedRAMP after requesting any additional information or materials from a cloud service provider beyond those required in this policy by sending a notification to info@fedramp.gov.

Note: This is an OMB policy; agencies are required to notify FedRAMP in OMB Memorandum M-24-15 section IV (a).